



# CVE-2014-7998

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2014-7998  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | psirt@cisco.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2014-11-15 02:59:00 UTC  |
| <b>Updated</b>         | 2017-09-08 01:29:00 UTC  |
| <b>Description</b>     | Cisco IOS on Aironet access points, when "dot11 aaa authenticator" debugging is enabled, allows remote attackers to caus |

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type     | Vendor | Product                   | Version | Update | Edition | Language |
|----------|--------|---------------------------|---------|--------|---------|----------|
| Hardware | Cisco  | Aironet 1040              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 1040              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 1140              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 1140              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 1260              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 1260              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3500              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3500              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600              | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600e             | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600e             | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600i             | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600i             | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600p             | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 3600p             | -       | All    | All     | All      |
| Hardware | Cisco  | Aironet 600 Office Extend | -       | All    | All     | All      |

|                  |       |                           |       |     |     |     |
|------------------|-------|---------------------------|-------|-----|-----|-----|
| Hardware         | Cisco | Aironet 600 Office Extend | -     | All | All | All |
| Hardware         | Cisco | Aironet Ap1100            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1100            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1130ag          | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1130ag          | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1131            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1131            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1200            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1200            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1230ag          | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1230ag          | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1240            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1240            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1240ag          | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1240ag          | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1300            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1300            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1400            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap1400            | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap340             | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap340             | 11.21 | All | All | All |
| Hardware         | Cisco | Aironet Ap340             | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap340             | 11.21 | All | All | All |
| Hardware         | Cisco | Aironet Ap350             | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap350             | 11.21 | All | All | All |
| Hardware         | Cisco | Aironet Ap350             | All   | All | All | All |
| Hardware         | Cisco | Aironet Ap350             | 11.21 | All | All | All |
| Operating System | Cisco | ios                       | -     | All | All | All |
| Operating System | Cisco | ios                       | -     | All | All | All |

## References

| Reference   | Source   | Link  | Ta |
|---|----------|---|----|
| Cisco Aironet EAP Debugging Denial of Service Vulnerability                         | CISCO    | <a href="https://tools.cisco.com">tools.cisco.com</a>                           | Ve |
| IBM X-Force Exchange  | XF       | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |    |
| Cisco Aironet EAP Processing Error Lets Remote Users Deny Service - SecurityTracker | SECTRACK | <a href="https://www.securitytracker.com">www.securitytracker.com</a>           |    |

|                          |         |  |    |
|--------------------------|---------|--|----|
| CVE Program record       | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>   | ca |
| NVD vulnerability detail | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a> | ca |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**